Public key identification method for authentication of bank cards or identity cards

Publication number: FR2763452
Publication date: 1998-11-20

Inventor: ARDITTI DAVID; GILBERT HENRI; STERN JACQUES; POINTCHEVAL DAVID
Applicant: FRANCE TELECOM (FR)

Classification:
- International: ***H04L9/32***; **H04L9/32**; (IPC1-7): H04L9/30; G07F7/12
- European: H04L9/32C
Application number: FR19970005831 19970513
Priority number(s): FR19970005831 19970513

Abstract of **FR2763452**

The procedure uses a public exponent of 3. The card holder randomly creates two exponents a and x, calculates r = g<3x> mod n and R = g<3a> mod n, then transmits r and R. The authenticator generates a random number e and transmits this to the card holder, who computes y = ea +x mod n and z = g<a> S mod n, then transmits y and z. The authenticator verifies that g<3y> is equal to R<e> r mod n and that z<3> is equal to R mod n.

(19) RÉPUBLIQUE FRANÇAISE

INSTITUT NATIONAL
DE LA PROPRIÉTÉ INDUSTRIELLE

PARIS

(11) **N° de publication :** **2 763 452**
(à n'utiliser que pour les commandes de reproduction)

(21) **N° d'enregistrement national :** **97 05831**

(51) Int Cl[6] : **H 04 L 9/30,** G 07 F 7/12

(12) DEMANDE DE BREVET D'INVENTION A1

(22) **Date de dépôt :** 13.05.97.

(30) **Priorité :**

(43) **Date de mise à la disposition du public de la demande :** 20.11.98 Bulletin 98/47.

(56) **Liste des documents cités dans le rapport de recherche préliminaire :** *Se reporter à la fin du présent fascicule*

(60) **Références à d'autres documents nationaux apparentés :**

(71) **Demandeur(s) :** *FRANCE TELECOM SOCIETE ANONYME* — FR.

(72) **Inventeur(s) :** ARDITTI DAVID, GILBERT HENRI, STERN JACQUES et POINTCHEVAL DAVID.

(73) **Titulaire(s) :**

(74) **Mandataire(s) :** SOCIETE DE PROTECTION DES INVENTIONS.

(54) PROCEDE D'IDENTIFICATION A CLE PUBLIQUE.

(57) Procédé d'identification d'un premier moyen (le vérifié) à l'aide d'un second moyen (le vérificateur).

Le procédé est du type à clé publique, où l'exposant public est égal à 3. Le vérifié tire au hasard deux exposants a et x, calcule $r = g^{3x} \bmod n$, et $R = g^{3a} \bmod n$ et transmet R et r. Le vérificateur tire au hasard un nombre e et le transmet au vérifié. Le vérifié calcule $y = ea + x \bmod n$ et $z = g^{ea}S \bmod n$ et transmet y et z. Le vérificateur vérifie que g^{3y} est égal à $R^{e}r \bmod n$ et que z^3 est égal à $RI \bmod n$.

Application dans la vérification de l'authenticité de divers supports comme les cartes bancaires.

FR 2 763 452 - A1

PROCEDE D'IDENTIFICATION A CLE PUBLIQUE

Domaine technique

La présente invention se rapporte à un procédé cryptographique d'identification, permettant à un support quelconque, appelé module d'identité (par exemple une carte à mémoire, un microprocesseur, un ordinateur, etc.), de prouver son identité à des moyens mettant en oeuvre une application, ou à un interlocuteur doté de moyens de vérification, et ceci grâce à un protocole mettant en jeu, sans les révéler, un ou des secret(s) contenu(s) dans le support.

Un protocole d'identification est donc un dialogue, à travers un réseau de télécommunications, entre deux entités : d'une part, une première entité qui veut prouver son identité et qui peut être, le cas échéant, équipée d'un terminal, (par exemple un ordinateur doté d'un lecteur de cartes à mémoire) et, d'autre part, une seconde entité capable de dialoguer avec la première et de réaliser certains calculs de vérification.

La première entité, dont on veut vérifier l'identité, sera appelée par la suite "le vérifié" (en anglais "the prover") et la seconde "le vérificateur" (en anglais "the verifier").

La présente invention se rapporte plus particulièrement à un procédé d'identification à clé publique, dans lequel le vérificateur n'a pas besoin de connaître les secrets contenus dans le module d'identité du vérifié, mais seulement des données non confidentielles (la clé publique) pour effectuer les calculs de vérification.

L'algorithme de chiffrement a clé publique dit RSA (des initiales de leurs auteurs RIVEST, SHAMIR, ADLEMAN) est décrit dans le brevet américain US-A-4,405,829. C'est actuellement l'algorithme à clé publique le plus utilisé. Il fournit des schémas de signature utilisables également à des fins d'identification.

Dans l'algorithme RSA, on choisit deux nombres premiers distincts p et q, et on forme leur produit n. On choisit également un entier e, qui est premier avec le plus petit commun multiple de (p-1) et (q-1) (ou, si l'on veut, qui est premier avec le produit (p-1) (q-1)). Pour chiffrer un message, préalablement mis sous forme numérique u, u étant compris entre 0 et n-1, on calcule la puissance e-ième de u dans l'anneau des entiers modulo n, soit $v = u^e \bmod n$. On rappelle que la valeur d'un entier x modulo un entier n est égale au reste de la division de x par n.

Pour déchiffrer un message tel que v, il faut extraire la racine e-ième du message chiffré v dans l'anneau des entiers modulo n. On montre que cette opération revient à élever le nombre v à la puissance d, d étant l'inverse de l'exposant e modulo le plus petit commun multiple des nombres (p-1) et (q-1). Si l'on ne connaît pas les facteurs premiers p et q, la détermination de d est impossible et, avec elle, l'opération de déchiffrement.

L'une des premières utilisations pratiques du procédé RSA à des fins d'identification a été la suivante : une autorité, responsable de la mise en place d'un système d'identification, émet une clé publique de type RSA, c'est-à-dire, en pratique, les

deux nombres n et e, cette clé étant commune à tout le système, et conserve les éléments secrets correspondants (p et q). Cette autorité dépose, dans chaque module d'identité des usagers du système, le couple constitué par :

- le numéro d'identification ID du module d'identité ;
- la racine e-ième (ou l'inverse de la racine e-ième), modulo n, d'un nombre obtenu à partir du numéro ID en appliquant à ID une fonction de redondance connue de tous (dont un exemple peut être trouvé dans la norme ISO 9796). Cette racine e-ième (ou son inverse), calculée par l'autorité d'émission à l'aide des éléments secrets qu'elle détient, est appelée "accréditation".

Les accréditations déposées dans les modules d'identité peuvent, en premier lieu, être utilisées à des fins d'identification passive (c'est-à-dire ne nécessitant aucun calcul de la part de celui qui veut prouver son identité).Le protocole se réduit alors, pour le vérificateur, aux opérations suivantes :

- lire le couple identité-accréditation contenu dans un module d'identité ;
- calculer la puissance e-ième de l'accréditation et s'assurer que le résultat de ce calcul et l'application de la fonction de redondance au numéro d'identification ID fournissent bien le même résultat.

Un telle identification passive montre au vérificateur que celui qui veut prouver son identité dispose de données qui ne peuvent avoir été émises que par l'autorité, ce qui limite, dans une certaine mesure, les usurpations d'identité. Mais rien n'interdit cependant à un pirate capable d'intercepter le protocole vérifié-vérificateur, ou à un vérificateur mal-

honnête, de réutiliser à son profit les données communiquées par le vérifié.

Malgré ce risque de fraude par réutilisation, l'identification passive décrite ci-dessus est largement utilisée dans le domaine bancaire et celui des cartes de télécommunication. Des précautions supplémentaires (listes noires, etc.) limitent dans une certaine mesure l'ampleur des fraudes par réutilisation.

Cependant, pour résoudre le problème de la fraude par réutilisation des données échangées, problème inhérent aux protocoles d'identification passifs, des protocoles d'identification actifs, c'est-à-dire nécessitant des calculs de la part de celui qui veut prouver son identité, ont été proposés. Parmi ces protocoles figurent non seulement l'utilisation de l'algorithme RSA pour signer une question aléatoire posée par le vérificateur, mais encore des schémas interactifs où le vérifié démontre au vérificateur qu'il possède une ou plusieurs accréditations du type de celles définies plus haut, et cela sans révéler cette (ou ces) accréditation(s). Parmi les schémas de ce type, les plus utilisés actuellement sont le schéma de FIAT-SHAMIR et le schéma de GUILLOU-QUISQUATER.

Le schéma d'identification de FIAT-SHAMIR est décrit dans le brevet US-A-4,748,668. Le schéma d'identification de GUILLOU et QUISQUATER est décrit dans le document FR-A-2 620 248 (ou son correspondant européen EP-A-0 311 470 ou son correspondant américain US-A-5,218,637).

Ces deux schémas consistent en une ou plusieurs itérations d'une variante de base à trois passes dans laquelle :

1. celui qui veut prouver son identité, (le vérifié) calcule la puissance e-ième modulo n d'un nombre aléatoire r qu'il a tiré, et en déduit un nombre x, appelé le témoin, qu'il envoie au vérificateur ;

2. le vérificateur tire au sort un nombre b, appelé la question, et l'envoie au vérifié ;

3. le vérifié calcule, par exemple, le produit du nombre aléatoire r par la puissance b-ième de son accréditation, soit $y = rS^b \bmod n$ et envoie le résultat y au vérificateur.

Le vérificateur peut calculer la puissance e-ième de y, et comme il connaît la puissance e-ième de l'accréditation S du vérifié, il est alors capable de vérifier la cohérence entre x, b et y.

Ces schémas présentent un double avantage pour l'identification active : d'une part, si l'on se contente d'un niveau d'insécurité (défini comme la probabilité maximale de succès d'un fraudeur) de l'ordre de 10^{-6}, ils sont nettement moins coûteux en temps de calcul qu'une signature RSA ; d'autre part, ces schémas sont, du moins dans leur version de base, à divulgation nulle de connaissance (en anglais "zero-knowledge"), ce qui entraîne que les échanges liés à un processus d'identification ne peuvent être d'aucun secours à un fraudeur pour la recherche des accréditations secrètes d'un utilisateur.

Deux configurations peuvent être envisagées pour la mise en oeuvre, côté vérifié, de schémas d'identification actifs démontrant la possession d'accréditations du type de ceux qui viennent d'être expo-

sés. Dans une première configuration, le module d'identité contenant les accréditations possède une puissance de calcul suffisante pour réaliser tous les calculs de son côté. Dans une seconde configuration le module d'identité contenant les accréditations n'effectue pas les calculs lui-même mais les fait réaliser dans un terminal (par exemple un micro-ordinateur capable de lire les accréditations dans le module d'identité).

La seconde configuration, bien qu'un peu moins sûre que la première, peut cependant être utile pour améliorer la sécurité de la vérification de modules d'identité initialement conçus pour une simple identification passive. Il est nécessaire de faire confiance au terminal utilisé côté vérifié, mais sous réserve que ce terminal soit intègre, aucune fraude provenant du réseau ou du vérificateur n'est possible.

Dans la présente invention, on s'intéresse plus particulièrement au problème de l'utilisation, selon la seconde configuration, de supports d'identité initialement conçus pour une identification passive, dans lesquels une unique accréditation correspondant à un exposant public e égal à 3 a été déposée : la majeure partie des cartes bancaires françaises, ainsi que d'autres supports d'identité (par exemple les cartes de télécommunications) sont de ce type.

Le procédé de GUILLOU- QUISQUATER est en théorie utilisable par le terminal côté vérifié, pour démontrer au vérificateur la possession de l'accréditation. Le procédé de GUILLOU-QUISQUATER, dans ce cas particulier, comprend les opérations suivantes :

a) deux grands nombres premiers p et q définissent l'entier n, produit de p par q ; le nombre n est rendu public ;

b) le support de celui qui doit prouver son identité contient une accréditation secrète S comprise entre 1 et n-1 ; le cube de l'accréditation modulo n, c'est-à-dire $I = S^3 \bmod n$, est rendu public ;

c) le support du vérifié est pourvu de moyens aptes à tirer au hasard un entier r compris entre 1 et n-1, et à calculer le cube de r modulo n, appelé le témoin x :

$$x = r^3 \bmod n ;$$

d) le vérifié transmet le témoin x au vérificateur ;

e) le vérificateur tire au sort un entier b inférieur à l'exposant 3, donc égal à 0, 1, ou 2 ; cet entier est appelé la question ;

f) le vérificateur transmet la question b au vérifié ;

g) le vérifié calcule le nombre y défini par :

$$y = rS^b \bmod n$$

h) le vérifié transmet ce nombre y au vérificateur ;

i) le vérificateur élève au cube le nombre y et, par ailleurs, calcule le produit du témoin x (qui lui a été transmis) par la puissance b de I (b qu'il a tiré et I qui est public) ; le vérificateur compare alors y^3 et $xI^b \bmod n$, s'il y a coïncidence, le vérifié a répondu correctement à la question et son authenticité est présumée.

La sécurité d'un tel schéma repose sur l'hypothèse même du schéma RSA : l'entier n étant

public ainsi que l'exposant 3, il est difficile, pour un tiers fraudeur, de remonter à r en prenant la racine cubique de x, sans connaître les facteurs p et q, dont n est le produit. Ne connaissant pas r, le tiers fraudeur ne peut répondre correctement à la question posée par le vérificateur.

Pour un tel procédé, ainsi que pour les autres schémas d'identification connus à ce jour, la situation où l'on ne dispose que d'une seule accréditation correspondant à un exposant public égal à 3 conduit à des protocoles très coûteux en communications. En effet, le niveau de sécurité d'un échange de base (témoin, question, réponse) que l'on peut réaliser dans les conditions citées est inférieur ou égal à 3 pour le schéma de GUILLOU-QUISQUATER. Pour parvenir à un niveau de sécurité convenable (insécurité inférieure à 2^{-16}), il faut donc répéter l'échange de base au moins une dizaine de fois, ce qui conduit à multiplier le nombre de bits à échanger entre vérifié et vérificateur par un facteur de dix au moins.

Le but de la présente invention est justement de remédier à cet inconvénient. Il s'agit de proposer un schéma, à la fois réaliste en temps de calcul et moins coûteux en nombre de bits échangés, permettant de démontrer la possession d'une accréditation correspondant à un exposant public égal à 3, sans la révéler.

Exposé de l'invention

Le procédé de l'invention est fondé sur l'hypothèse selon laquelle, pour tout entier n, si l'on connaît deux nombres g et y compris entre 0 et n-1, il est difficile de calculer α, s'il existe, tel que :

$$y = g^{\alpha} \bmod n.$$

Sous cette hypothèse, l'invention se définit comme suit il s'agit d'un procédé d'identification d'un support appelé "le vérifié", par des moyens appelés "le vérificateur", ce support et ces moyens étant équipés de moyens de calcul et de mémorisation appropriés, le vérifié et le vérificateur possédant en commun :

- un nombre entier n, produit de deux nombres premiers (p,q),
- un nombre λ qui est le plus petit facteur premier impair de (p-1)(q-1),
- un nombre k, paramètre de sécurité inférieur à λ,
- un nombre entier g compris entre 2 et n-1 et d'ordre λ,

le vérifié possédant en outre un nombre secret S égal à $g^{v} \bmod n$, où v est un nombre secret, le secret S définissant l'identité du vérifié, le vérificateur ayant en outre connaissance de la puissance 3 modulo n de ce secret, soit $I = S^{3} \bmod n$,

procédé dans lequel le vérifié et le vérificateur mettent en oeuvre leurs moyens de calcul et de mémorisation pour effectuer les opérations successives suivantes :

Phase A ; le vérifié :

Aa) tire au hasard un premier exposant α entier compris entre 0 et λ-1,

Ab) tire au hasard un second exposant x entier compris entre 0 et λ-1,

Ac) calcule un nombre r égal à la puissance 3x du nombre g modulo n, soit :

$$r = g^{3x} \bmod n$$

Ad) calcule un nombre R égal à la puissance 3α du nombre g modulo n, soit :

$$R = g^{3\alpha} \bmod n,$$

Ae) transmet les nombres r et R au vérificateur,

Phase B ; le vérificateur :

Ba) tire au hasard un nombre e entier compris entre 0 et λ-1,

Bb) transmet au vérifié le nombre e,

Phase C ; le vérifié :

Ca) calcule un nombre y égal à eα + x modulo λ,

Cb) calcule un nombre z égal à $g^{\alpha}S$ modulo n,

Cc) transmet les nombres y et z au vérificateur,

Phase D ; le vérificateur :

Da) calcule le produit de R^e par r modulo n et la puissance y de g^3, soit g^{3y}, et vérifie si les deux résultats sont égaux, c'est-à-dire :

$$g^{3y} \stackrel{?}{=} R^e r \bmod n,$$

Db) calcule le produit de R par l'identité publique I et le cube de z et vérifie si les deux résultats obtenus sont égaux, c'est-à-dire :

$$z^3 \stackrel{?}{=} RI \bmod n,$$

l'identification du vérifié par le vérificateur étant acquise si les deux vérifications Da) Db) sont avérées.

Le nombre λ doit être suffisamment grand. Le nombre k peut être par exemple de l'ordre de 2^{20} pour une insécurité inférieure à 2^{-19}.

Le tableau ci-dessous résume les différentes opérations.

TABLEAU I

Vérifié		Vérificateur
0	n, k, g, I, λ	n, k, g, I
A	$S = g^y \bmod n$ $\alpha < \lambda$ $x < \lambda$ $r = g^{3x} \bmod n$ $R^2 = g^{3\alpha} \bmod n$ $\xrightarrow{R,r}$	
B	$\xleftarrow{e}$	$e < k$
C	$y = e\alpha + x \bmod \lambda$ $z = g^a S \bmod n$ $\xrightarrow{y,z}$	
D		$g^{3y} \overset{?}{=} R^e r \bmod n$ $z^3 \overset{?}{=} RI \bmod n$

La bande horizontale marquée 0 indique les données connues des deux entités, à savoir, le nombre n, le nombre k, le nombre g, et le cube du secret, soit I.

La bande horizontale A rassemble les premières opérations effectuées par le vérifié (opérations Aa à Ae dans la définition précédente).

La bande horizontale B montre l'opération suivante effectuée par le vérificateur.

La bande horizontale C rassemble les opération effectuées à nouveau par le vérifié (opérations Ca, Cc)

La bande horizontale D, enfin, rassemble les deux dernières opération effectuées par le vérificateur.

Un tel procédé permet bien de vérifier l'authenticité d'un possesseur d'accréditation. En effet, si le vérifié connaît le secret S il pourra répondre correctement à la question posée par le vérificateur puisqu'il pourra calculer la quantité $z = g^{\alpha}S \bmod n$.

Réciproquement, pour être accepté, le vérifié doit permettre la vérification des deux équations Da, Db. Supposons qu'il soit capable de les satisfaire avec une probabilité supérieure à 2/k. Cela signifie que, après s'être engagé avec R et r, le vérifié sait répondre à au moins deux questions e et e' différentes modulo 2. Soient (y,z) et (y',z') les réponses respectives. Alors, $r = g^{3y}R^{-e} = g^{3y'}R^{-e'} \bmod n$ et $z^3 = z'^3 = RI \bmod n$. Par conséquent, $z = z'$ et $(g^{y-y'})^3 = R^{e-e'} \bmod n$. Ainsi, comme λ est premier et supérieur à e-e', l'égalité de Bezout fournit u et w tels que $u\lambda + w(e-e') = 1$. Alors, $(g^{y-y'})^{3w} = R^{w(e-e')} = R.R^{-u\lambda} \bmod n$. Comme e-e' est impair et inférieur à λ, le plus petit facteur impair de $(p-1)(q-1)$, alors e-e', admet un inverse, f modulo $(p-1)(q-1)$. Par conséquent, $R = (g^{(y-y')})^{3f} \bmod n$. Or, g est d'ordre λ, donc $R^{\lambda} = 1 \bmod n$. Ce qui entraîne, $R = (g^{w(y-y')})^3 \bmod n$. Par suite,

$$I = (zg^{-w(y-y')})^3 \bmod n.$$

Le vérifié doit donc nécessairement être en possession de l'accréditation S, racine cubique de I.

On peut voir également que même un malfaiteur utilisant toutes les techniques frauduleuses imaginables ne pourra obtenir une quelconque information sur l'accréditation du vérifié, et donc se faire ensuite passer pour lui.

En effet, ce protocole est à divulgation nulle de connaissance. Il est donc possible de simuler une interaction entre le vérifié et n'importe quel vérificateur, sans connaître le secret S. Soit σ la stratégie, aléatoire ou non, d'un vérificateur. C'est une fonction qui prend en entrée un couple (R,r), et retourne une question e. Le simulateur :

1. choisit ε compris entre 0 et k-1, ainsi que y et t compris entre 0 et λ-1,
2. calcule $z = g^t \bmod n$, $R = z^3 I^{-1} \bmod n$ et $r = g^{3y} R^{-e} \bmod n$,
3. interroge la stratégie du vérifieur : $e = \sigma(R,r)$,
4. si $e = \varepsilon$, on retourne à l'opération 1, sinon le simulateur écrit (R,r,e,y,z).

Le procédé défini est donc sûr, même face à des attaques actives. Il est à divulgation nulle de connaissance avec une probabilité d'acceptation d'un tricheur inférieure à 2/k après une itération.

REVENDICATIONS

1. Procédé d'identification d'un support appelé "le vérifié", par des moyens appelés "le vérificateur", ce support et ces moyens étant équipés de moyens de calcul et de mémorisation appropriés, le vérifié et le vérificateur possédant en commun :

- un nombre entier n, produit de deux nombres premiers (p,q),
- un nombre λ qui est le plus petit facteur premier impair de (p-1)(q-1),
- un nombre k, paramètre de sécurité inférieur à λ,
- un nombre entier g compris entre 2 et n-1 et d'ordre λ,

le vérifié possédant en outre un nombre secret S égal à $g^v \bmod n$, où v est un nombre secret, le secret S définissant l'identité du vérifié, le vérificateur ayant en outre connaissance de la puissance 3 modulo n de ce secret, soit $I = S^3 \bmod n$,

procédé dans lequel le vérifié et le vérificateur mettent en oeuvre leurs moyens de calcul et de mémorisation pour effectuer les opérations successives suivantes :

Phase A ; le vérifié :

Aa) tire au hasard un premier exposant α entier compris entre 0 et λ-1,

Ab) tire au hasard un second exposant x entier compris entre 0 et λ-1,

Ac) calcule un nombre r égal à la puissance 3x du nombre g modulo n, soit :

$$r = g^{3x} \bmod n$$

Ad) calcule un nombre R égal à la puissance 3α du nombre g modulo n, soit :

$$R = g^{3\alpha} \bmod n,$$

Ae) transmet les nombres r et R au vérificateur,

Phase B ; le vérificateur :

Ba) tire au hasard un nombre e entier compris entre 0 et λ-1,

Bb) transmet au vérifié le nombre e,

Phase C ; le vérifié :

Ca) calcule un nombre y égal à eα + x modulo λ,

Cb) calcule un nombre z égal à $g^{\alpha}S$ modulo n,

Cc) transmet les nombres y et z au vérificateur.

Phase D ; le vérificateur :

Da) calcule le produit de R^e par r modulo n et la puissance y de g^3, soit g^{3y}, et vérifie si les deux résultats sont égaux, c'est-à-dire :

$$g^{3y} \stackrel{?}{=} R^e r \bmod n,$$

Db) calcule le produit de R par l'identité publique I et le cube de z et vérifie si les deux résultats obtenus sont égaux, c'est-à-dire :

$$z^3 \stackrel{?}{=} RI \bmod n,$$

l'identification du vérifié par le vérificateur étant acquise si les deux vérifications Da) Db) sont avérées.

2. Procédé selon la revendication 1, dans lequel le support du vérifié est une carte à mémoire.

REPUBLIQUE FRANÇAISE

INSTITUT NATIONAL
de la
PROPRIETE INDUSTRIELLE

RAPPORT DE RECHERCHE PRELIMINAIRE

établi sur la base des dernières revendications déposées avant le commencement de la recherche

N° d'enregistrement national

FA 542405
FR 9705831

DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie	Citation du document avec indication, en cas de besoin, des parties pertinentes	Revendications concernées de la demande examinée
D,A	EP 0 311 470 A (ETAT FRANCAIS) * colonne 6, ligne 19 - ligne 60 * * colonne 9, ligne 14 - colonne 10, ligne 20 * -----	1

DOMAINES TECHNIQUES RECHERCHES (Int.Cl.6)

H04L

1

Date d'achèvement de la recherche: 9 mars 1998

Examinateur: Holper, G

CATEGORIE DES DOCUMENTS CITES

X : particulièrement pertinent à lui seul
Y : particulièrement pertinent en combinaison avec un autre document de la même catégorie
A : pertinent à l'encontre d'au moins une revendication ou arrière-plan technologique général
O : divulgation non-écrite
P : document intercalaire

T : théorie ou principe à la base de l'invention
E : document de brevet bénéficiant d'une date antérieure à la date de dépôt et qui n'a été publié qu'à cette date de dépôt ou qu'à une date postérieure.
D : cité dans la demande
L : cité pour d'autres raisons

.....

& : membre de la même famille, document correspondant

EPO FORM 1503 03.82 (P04C13)